Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-10 (canceled)

Claim 11 (original): A method of securely conveying data, the method comprising the steps of:

assembling a set of authorization parameters associated with the data;

computing a first checksum of the set of authorization parameters;

generating a first cryptographic key substantially randomly;

using the first cryptographic key to symmetrically encrypt the set of authorization parameters, so as to produce an encrypted set of authorization parameters;

encrypting a combination of the first cryptographic key and the first checksum, so as to produce a header value that can be decrypted using a second cryptographic key; and

providing the header value, together with the data, for access by a receiving end.

Claim 12 (original): The method of claim 11, further comprising the following steps performed at the receiving end:

using the second cryptographic key to decrypt the header value, so as to produce an decrypted header value;

retrieving the first cryptographic key and first checksum from the decrypted header value;

using the first cryptographic key to decrypt the encrypted set of authorization parameters;

computing a second checksum of the set of authorization parameters;

comparing the second checksum with the first checksum, and refusing to access the data if the second checksum does not match the first checksum; and

using the set of authorization parameters to verify authorization to access the data.

Claim 13 (original): The method of claim 12, further comprising encrypting the data before providing the data and header value for access by the receiving end.

Claims 14-15 (canceled).

Claim 16 (original): A method of securely communicating a data product, while allowing the data product to be used in connection with at least one authorized entity, the at least one authorized entity having an associated identification code, the method comprising:

symmetrically encrypting at least a portion of the data product using a first cryptographic key, thereby producing an encrypted portion of the data product that can be symmetrically decrypted using the first cryptographic key;

establishing an authorization key including verification information;

computing a first value as a first function of input parameters including (i) the identification code and (ii) a second value;

combining the first value with the first cryptographic key to produce a third value;

adding the third value to the authorization key;

thereafter using the first value as a second cryptographic key to symmetrically encrypt the authorization key, so as to produce an encrypted authorization key that can be decrypted using the first value;

encrypting at least the second value to produce an encrypted value that can be decrypted using a third cryptographic key; and

providing to a receiving-end at least (i) the encrypted value, (ii) the encrypted authorization key, and (iii) the encrypted portion of the data product,

whereby, if the receiving end has access to the third cryptographic key and the input parameters, the receiving end may be able to uncover the first authorization key and the cryptographic key and may therefore be able to access the verification information and decrypt the encrypted portion of the data product.

Claim 17 (original): The method of claim 16, wherein the data product comprises geographical information, the authorized entity comprises a navigation system, and the identification code comprises a navigation system ID.

Claim 18 (original): The method of claim 16, wherein the data product comprises geographical information, the authorized entity comprises a data storage device, and the identification code comprises a storage device ID.

Claim 19 (original): The method of claim 16, wherein the first function comprises a hash function.

Claim 20 (original): The method of claim 19, wherein the input parameters further include a predetermined segment of the encrypted portion of the data product.

Claim 21 (original): The method of claim 16, wherein combining the first value with the first cryptographic key to produce a third value comprises computing an XOR sum of the first value and the first cryptographic key.

Claim 22 (original): The method of claim 16, wherein encrypting at least the second value to produce an encrypted value that can be decrypted with a third cryptographic key comprises:

combining the second value with a checksum of the authorization key; and

using a public key encryption algorithm to encrypt the second value

Claim 23 (original): The method of claim 16, further comprising the following steps:

receiving at the receiving-end (i) the encrypted value, (ii) the encrypted authorization key, and (iii) the encrypted portion of the data product,

using the third cryptographic key to decrypt the encrypted value

computing the first value as the first function of the input parameters;

using the first value as the second cryptographic key to symmetrically decrypt the encrypted authorization key;

extracting the third value from the authorization key;

using the third value and the first value to generate the first cryptographic key; and

using the first cryptographic key to symmetrically decrypt the encrypted portion of the data product.

Claim 24 (original): The method of claim 23, further comprising, at the receiving-end, verifying the checksum of the authorization key.

Claim 25 (original): The method of claim 23, wherein using the third value and the first value to generate the first cryptographic key comprises computing an XOR sum of the third value and the first value.

Claim 26 (original): The method of claim 23, further comprising the step of validating use of the data product by reference to the verification information.

Claim 27 (original): A method of securing a data product against unauthorized use, while allowing the data product to be used in connection with at least one authorized entity, the at least one authorized entity having an associated identification code, the method comprising:

symmetrically encrypting at least a portion of the data product using a first cryptographic key, thereby producing an encrypted portion of the data product that can be symmetrically decrypted using the first cryptographic key;

establishing an authorization key including verification information;

computing a first value as a first function of input parameters including (i) the identification code and (ii) a second value;

combining the first value with the first cryptographic key to produce a third value;

adding the third value to the authorization key;

thereafter using the first value as a second cryptographic key to symmetrically encrypt the authorization key, so as to produce an encrypted authorization key that can be decrypted using the first value; and

encrypting at least the second value to produce an encrypted value that can be decrypted using a third cryptographic key.

Claim 28 (original): The method of claim 27, further comprising randomly generating the first cryptographic key.

Claim 29 (original): The method of claim 27, wherein the portion of the data product comprises the entire database.

Claim 30 (original): The method of claim 27, wherein the portion of the data product comprises information required to understand contents of the data product.

Claim 31 (original): The method of claim 30, wherein the information required to understand contents of the data product is selected from the group consisting of (i) database decompression information and (ii) pointers.

Claim 32 (original): The method of claim 27, wherein the data product comprises geographic information.

Claim 33 (original): The method of claim 27, wherein the data product comprises geographic information, the authorized entity comprises a navigation system, and the identification code comprises a navigation system ID.

Claim 34 (original): The method of claim 27, wherein the data product comprises geographic information, the authorized entity comprises a data storage device, and the identification code comprises a storage device ID.

Claim 35 (original): The method of claim 27, wherein the first function comprises a hash function.

Claim 36 (original): The method of claim 27, wherein the input parameters further include a predetermined segment of the encrypted portion of the data product.

Claim 37 (original): The method of claim 27, wherein combining the first value with the first cryptographic key to produce a third value comprises computing an XOR sum of the first value and the first cryptographic key.

Claim 38 (original): The method of claim 27, wherein encrypting at least the second value to produce an encrypted value that can be decrypted with a third cryptographic key comprises:

combining the second value with a checksum of the authorization key; and

using a public key encryption algorithm to encrypt the second value.

Claim 39 (original): A system for securing a data product against unauthorized use, while allowing the data product to be used in connection with at least one authorized entity, the system comprising:

a processor;

a data storage medium; and

a set of machine language instructions stored in the data storage medium and executable by the processor to carry out the method steps of claim 27.